AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An apparatus for selectively encrypting data for transmission over a network in packets between a server and a client, the apparatus comprising:

a parser configured to parse a payload portion of the data in a packet from a non-payload portion of the packet data;

an encrypter configured to determine if the payload portion of the packet data is to be encrypted by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, to encrypt the payload portion of the packet data; and

a data combiner configured to combine the encrypted payload portion of the packet data with the non-payload portion of the packet data, wherein the non-payload portion of the packet data includes more than routing information.

2. (Currently Amended) The apparatus of claim 1, wherein the packet data includes streaming data.

3. (Canceled)

4. (Currently Amended) The apparatus of claim 1, wherein the non-payload portion of the packet data includes at least one of a header, control data and routing data.

5. (Currently Amended) The apparatus of claim 1, further comprising a transmitter configured to send the combined payload and non-payload portions of the packet data over the network to the client.

6. (Currently Amended) The apparatus of claim 1, further comprising a receiver configured to receive the data from the server before the data is sent in the packet over the network to the client.

7. (Previously Presented) The apparatus of claim 1, further comprising a device configured to establish a data stream between the server and the client.

8. (Previously Presented) The apparatus of claim 1, further comprising a key negotiator configured to negotiate an encryption key with the client.

9. (Previously Presented) The apparatus of claim 8, wherein key negotiation and key exchange occur during transmission of a stream.

10. (Previously Presented) The apparatus of claim 9, wherein the encrypter is transparent to the server.

11. (Previously Presented) The apparatus of claim 8, wherein key negotiation can determine if the encryption key is current.

12. (Currently Amended) The apparatus of claim 1, further comprising a decrypter configured to decrypt the encrypted payload portion of the packet data at the client.

13. (Currently Amended) The apparatus of claim 1, wherein the parser is further configured to parse the packet data into different portions based on a media format.

14. (Currently Amended) The apparatus of claim 1, wherein the encrypter is further configured to encrypt the payload portion of the packet data based on a media format.

15. (Currently Amended) The apparatus of claim 1, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the payload portion of the packet data, wherein the pluggable core enables the encryption algorithm to be readily changed.

16. (Previously Presented) The apparatus of claim 1, wherein the apparatus in implemented on an encryption bridge.

17. (Currently Amended) A method for selectively encrypting data in a packet received from a data source, the data including payload and non-payload portions which differ from each

other in at least one characteristic, the received data to be subsequently sent over a network to a client, the method comprising:

parsing the received packet data into portions including the payload and non-payload portions;

determining if the payload portion is to be encrypted based on a format of the payload portion of the packet data by examining the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting the payload portion of the received packet data; and

sending the received packet data including the encrypted payload portion and the non-payload portion of the received packet data over the network to the client.

18. (Previously Presented) The method of claim 17, wherein the data source is a server.

19. (Previously Presented) The method of claim 17, further comprising determining whether a stream is established between a server and the client.

20. (Previously Presented) The method of claim 17, further comprising negotiating an encryption key with the client.

21. (Currently Amended) The method of claim 20, wherein the received packet data from the data source is streaming data sent during a streaming session and the negotiating of the encryption key is carried out during the streaming session.

22. (Currently Amended) The method of claim 20, wherein the received packet data from the data source is streaming data sent during a streaming session, the method further comprising examining the client during the streaming session and terminating the streaming session if the encryption key on the client is invalid.

23. (Previously Presented) The method of claim 20, wherein the encryption key is negotiated with a decryption shim on the client.

24. (Currently Amended) The method of claim 17, further comprising determining whether the received packet data is streaming data.

25. (Currently Amended) The method of claim 24, further comprising parsing, encrypting and sending the packet data if the packet data is streaming data and sending the packet data if the packet data is not streaming data.

26. (Previously Presented) The method of claim 17, further comprising determining whether a shim is present on the client.

27. (Previously Presented) The method of claim 26, further comprising sending a shim to the client if it is determined that the shim is not present on the client.

28. (Previously Presented) The method of claim 17, further comprising determining whether an encryption key on the client is current.

29. (Currently Amended) The method of claim 17, wherein the packet data includes at least one of a header, control data and routing data.

30. (Canceled)

31. (Currently Amended) The method of claim 17, wherein the packet data received from the data source for sending to the client is a stream of packets, the method further comprising determining whether a particular packet is the last packet in a data stream.

32. (Currently Amended) The method of claim 31, further comprising receiving feedback from a decryption shim on the client if it is determined that the particular packet is not the last packet in the data stream.

33. (Previously Presented) The method of claim 17, further comprising determining whether the client is compromised.

34. (Currently Amended) The method of claim 33, further comprising continuing parsing, encrypting and sending the packet data into the payload and non-payload portions if it is determined that the client is not compromised.

35. (Previously Presented) The method of claim 33, further comprising terminating the sending to the client if it is determined that the client is compromised.

36. (Currently Amended) A method for streaming data at a client, the data including payload and non-payload portions which differ from each other in at least one characteristic, the streaming data is included in a plurality of packets having been sent over a network to the client from an encryption source, the method comprising:

receiving the packet data sent over the network;

parsing the packet data into portions including the payload and non-payload portions;

if the payload portion of the packet data is encrypted based on a format of the payload portion of the packet data, as determined by an examination of the payload portion of the packet data to recognize a predefined data type, decrypting the payload portion of the packet data; and

passing the decrypted payload portion of the packet data to a higher level of operations for play in the client.

37. (Currently Amended) The method of claim 36, further comprising prior to the parsing, determining whether the packet data is an unencrypted stream.

38. (Currently Amended) The method of claim 37, further comprising passing the packet data to a higher level of operations without parsing and decrypting ~~when~~ if it is determined that the packet data is an unencrypted stream.

39. (Previously Presented) The method of claim 36, further comprising negotiating a decryption key with the encryption source.

40. (Previously Presented) The method of claim 39, wherein the streaming data is sent from the encryption source during a streaming session and said negotiating the decryption key is carried out during the streaming session.

41. (Previously Presented) The method of claim 39, further comprising terminating a stream if the decryption key is invalid.

42. (Canceled)

43. (Currently Amended) The method of claim 36, wherein the packet data is sent from the encryption source over the network as a stream of data packets, the method further comprising determining whether a particular packet received by the client is a last packet in a data stream.

44. (Currently Amended) The method of claim 43, further comprising sending feedback to the encryption source if it is determined that the particular packet is not the last packet in the data stream.

45. (Previously Presented) The method of claim 36, further comprising determining whether the client is compromised.

46. (Currently Amended) The method of claim 45, further comprising continuing the parsing, decrypting and passing the packet data as aforesaid if it is determined that the client is not compromised.

47. (Previously Presented) The method of claim 45, further comprising terminating a streaming session if it is determined that the client is compromised.

48. (Currently Amended) The apparatus of claim 1, wherein the payload packet data includes multimedia data.

49. (Currently Amended) The apparatus of claim 1, wherein the parser is further configured to parse the packet data into different portions based on a data protocol used to transmit a data stream of packets.

50. (Currently Amended) The apparatus of claim [[1]] 36, wherein the parser parses the packet data based on [[the]] a data protocol.

51. (Currently Amended) The method of claim 41, wherein the terminating of the encrypted stream includes sending a feedback signal to the encryption source instructing to stop sending the packet data over the network.

52. (Previously Presented) The method of claim 36, further comprising terminating a streaming session based on a determination that the client is compromised.

53. (Currently Amended) A method for selectively encrypting data for transmission over a network, the method comprising:

examining the data of each received packet to identify a plurality of portions that include at least a payload portion and a non-payload portion;

determining if at least one of the payload portion is to be to encrypted by examining the at least one payload portion to recognize a predefined data type, and if the at least one payload portion is to be encrypted, encrypting the at least one payload portion; and

at least another portion of the packet to remain unencrypted, wherein the plurality of portions of encrypted payload and non-payload for a packet being combined after such encryption determination.

54. (Currently Amended) The method of claim 53, wherein the packet data is received from a data source, wherein the packet data includes streaming data and wherein the at least one data portion of a packet to remain unencrypted includes at least one of a header, control data and routing data.

55. (Currently Amended) The method of claim 54, wherein the streaming data is included in the at least one data portion of the packet to remain unencrypted.

56. (Currently Amended) The method of claim 55, further comprising:

transmitting the combined packet data over the network to a client; and

negotiating and exchanging a key with the client before the combined data is transmitted over the network to the client, the key enabling the client to decrypt the encrypted portion of the packet data for play on the client.

57. (Previously Presented) The method of claim 56, wherein the streaming data is sent during a streaming session and wherein the negotiating and exchanging the key is carried out during the streaming session.

58. (Previously Presented) The method of claim 57, further comprising examining the client during the streaming session and terminating the streaming session if the key on the client is invalid.

59. (Currently Amended) The method of claim 58, wherein the data source is a server and the examining of the packet data is carried out on an encryption bridge between the server and the network so that the examining of the packet data, encrypting and combining of the plurality of data portions is transparent to the server.

60. (Previously Presented) The method of claim 59, wherein the key negotiating and exchanging and the decryption using the key is carried out using a shim on the client, the shim being configured so that the negotiating and exchanging of the key thereby and the decrypting of the data thereby is transparent to the client.

61. (Currently Amended) An apparatus for selectively encrypting streaming data packets received from a streaming data source for transmission over a network to a client, the apparatus comprising:

a parser configured to parse a plurality of portions of the streaming data packets, wherein the plurality of portions include a payload portion and a non-payload portion in each of the streaming data packets;

an encrypter configured to encrypt at least [[a]] the payload portion if it is determined, based on an examination of a format of the [[the]] payload portion to recognize a predefined data type, payload portion is to be encrypted, but not encrypt at least one other data portion of the plurality of data portions; and

a data combiner configured to combine the encrypted payload portion with at least one unencrypted non-payload data portion.

62. (Currently Amended) The apparatus of claim 61, further comprising a negotiator, wherein the negotiator negotiates and exchanges a key with the client before the combined packet data is transmitted over the network to the client, the key enabling the client to decrypt the encrypted payload portion of the packet data for play on the client.

63. (Previously Presented) The apparatus of claim 62, wherein the streaming data is sent from the streaming data source during a streaming session.

64. (Previously Presented) The apparatus of claim 63, further configured to perform actions including examining the client during the streaming session and terminating the streaming session if the client has been compromised.

65. (Currently Amended) The apparatus of claim 61, wherein the at least one unencrypted data portion of the packet data includes at least one of a header, control data and routing data.

66. (Previously Presented) The apparatus of claim 61, wherein the streaming data source is at least one server.

67. (Currently Amended) An apparatus for selectively encrypting data received from a data source for transmission in packets over a network to a client, comprising:

a parser configured to parse at least two portions of the packet data, at least one of the two portions of the packet data including more than routing information for a packet;

an encrypter configured to determine if ~~only one~~ a payload portion of the packet data is to be encrypted based on an examination of ~~only~~ the ~~one~~ payload portion the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting ~~only~~ the payload ~~one~~ portion of packet data not including the routing information for the packet; and

a data combiner configured to combine the parsed at least two portions of the packet data following encryption of the ~~one~~ payload portion of data not including the routing information for the packet.

68. (Currently Amended) The apparatus of claim 67, wherein [[the]]an unencrypted portion of the packet data includes at least one of a header and control data.

69. (Previously Presented) The apparatus of claim 68, wherein the parser parses the data into different portions based on a data protocol used to transmit the data.

70. (Currently Amended) The apparatus of claim 68, wherein the portion of the packet data to be encrypted includes media data encoded in a media format and wherein the encrypter encrypts the packet data to be encrypted based on the media format.

71. (Currently Amended) The apparatus of claim 70, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the packet data, the pluggable core being replaceable to enable the encryption algorithm to be readily changed.

72. (Previously Presented) The apparatus of claim 71, wherein the apparatus is implemented on an encryption bridge.

73. (Currently Amended) An apparatus for selectively encrypting data received from a data source during a downloading operation, the data being received from the data source for

transmission in packets over a network to a client receiving the downloaded packetized data, comprising:

a parser configured to parse at least two portions of the data in a packet, wherein the packet data includes a payload portion and a non-payload portion;

an encrypter configured to determine if [[a]]the payload portion of the packet data is to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined based on an examination of the payload portion of the packet data to recognize a predefined data type, and if it is to be encrypted, encrypting ~~only~~ the payload portion of the packet data; and

a data combiner configured to combine the encrypted payload portion of the packet data with an unencrypted portion of packet data for transmission over the network.

74. (Currently Amended) The apparatus as defined in claim 73, wherein the downloaded data is included in the encrypted payload portion of the packet data.

75. (Currently Amended) The apparatus of claim 74, wherein the unencrypted portion of packet data includes at least one of a header, control data and routing data.

76. (Currently Amended) The apparatus of claim 75, further comprising a key negotiator configured to perform actions including negotiating and exchanging a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of data.

77. (Canceled)

78. (Currently Amended) An apparatus for selectively encrypting data, received from a data source during a downloading operation and for selectively encrypting data received in packets from a data source during a streaming operation, the packet data being received from the data source for transmission over a network to a client receiving the downloaded or streaming data, comprising:

a means for parsing at least two portions of the data included in a packet, wherein the packet data comprises at least a payload portion and a non-payload portion;

a means for determining if [[a]]the payload portion of the at least two portions of data is to be encrypted based on a format of the one portion of packet data that is determined by recognizing a predefined data type in the payload portion of the at least two portions, and if the a payload portion of data is to be encrypted, employing a means for encrypting only the payload portion of the at least two portions of data; and

a means for combining the encrypted payload portion of the packet data with [[the]] at least the unencrypted portion of the packet data for transmission over the network.

79. (Currently Amended) The apparatus of claim 78, wherein during the streaming operation, the streaming data is included in the packet data portion that is to be encrypted.

80. (Currently Amended) The apparatus as defined in claim 79, further comprising a key negotiating means configured to negotiate and exchange a key with the client before the streaming data is sent over the network to the client, the key enabling the client to decrypt the encrypted payload portion of the packet data for play on the client.

81. (Canceled)

82. (Previously Presented) The apparatus of claim 78, further comprising a client examining means configured to examine the client during a streaming session and terminate the streaming session if the client has been compromised.

83. (Currently Amended) The apparatus of claim 82, wherein the packet data portion that is not encrypted includes at least one of a header, control data and routing data.

84. (Currently Amended) The apparatus of claim 78, wherein during a downloading operation, the downloaded data is included in the packet data portion that is to be encrypted.

85. (Previously Presented) The apparatus of claim 84, wherein the data portion that is not encrypted includes at least one of a header, control data and routing data.

86. (Currently Amended) A shim deployed on a client, the shim comprising:

a data receiver configured to receive partially encrypted packet data transmitted to the client, wherein another device parsed the packet data into a payload portion and a non-payload portion and determined [[a]]the payload portion of the packet data to be encrypted based on a format of the payload portion of the packet data, wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type[[,]];

a parser configured to parse the partially encrypted packet data to select the payload portion of the packet data to be decrypted;

a decrypter configured to decrypt the payload portion of the packet data selected for decrypting by the parser; and

a data transmitter configured to send the decrypted packet data to a higher level operation resident on the client.

87. (Currently Amended) The shim of claim 86, wherein an encrypted portion of the transmitted packet data includes media data, the data transmitter being further configured to send the decrypted media data to a media player resident on the client.

88. (Previously Presented) The shim of claim 87, wherein the media data is streaming media transmitted to the client during a streaming session.

89. (Currently Amended) The shim of claim 88, wherein the unencrypted portion of the packet data includes at least one of a header, control data and routing data.

90. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected.

91. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected.

92. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected.

93. (Previously Presented) The shim of claim 88, further comprising an analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected.

94. (Currently Amended) The shim of claim 88, further comprising a key negotiator configured to negotiate and exchange a key with the client before the packet data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of the packet data for play on the client.

95. (Currently Amended) The shim of claim 88, wherein the streaming data is sent to the client from an encryption source, the shim further including a key negotiator configured to negotiate and exchange a key with the encryption source, the key being used by the decrypter to decrypt the encrypted portion of the packet data.

96. (Previously Presented) The shim of claim 95 wherein the key negotiator is further configured to carry out the negotiating and exchanging of the key with the encryption source during the streaming session.

97. (Currently Amended) A method for providing data in packets over a network, comprising:

determining a plurality of portions of [[the]]data in a packet that includes a payload portion and a non-payload portion;

determining if at least [[a]]the payload portion of the plurality of portions of the packet data is to be encrypted based an examination of the payload portion, wherein the examination is to recognize a predefined data type and if the payload portion is to be encrypted, selectively encrypting the payload portion in the plurality of portions, wherein at least one other non-payload portion remains unencrypted;

authenticating a client to receive the packet that includes the selectively encrypted payload portion; and

transmitting the packet that includes the selectively encrypted payload portion to the authenticated client.

98. (Previously Presented) The method of claim 97, wherein authenticating the client further comprises the client accepting a shim transmitted from a server that is selectively encrypting the payload portion, and wherein the shim is configured to send back a confirmation.

99. (Previously Presented) The method of claim 97, wherein authenticating the client further comprises the client transmitting a self-generated certificate.